LECTURE 27: QUOTIENT MODULES & MODULE HOMOMORPHISMS

I'll begin by wrapping up our study of §10.1 of D&F.

Proposition 1 (Submodule Criterion)
Let R be a ring and let M be an R-module. A subset N of M is a submodule of M iff

(1.) $N \neq \emptyset$, and

(2.) $x + ry \in N$ for all $r \in R$ and for all $x, y \in N$

Proof: $\Rightarrow$] If N is submodule then $0 \in N \neq \emptyset$ and $x + ry \in N$ for all $r \in R$ and $\forall x, y \in N$ since N is submodule. Thus (1) and (2.) hold.

$\Leftarrow$] Suppose (1.) and (2.) are true. Let $x, y \in N$ and note $r = -1$ gives $x + ry = x - y \in N$ and $x - x = 0 \in N \neq \emptyset$ thus N is subgroup under $+$. Moreover, $ry \in N$ for any $r \in R$ thus N is a R-module. //

ALGEBRAS

It's finally happening, let's define "algebra"

Def^{n}/ Let R be a commutative ring with 1. An R-algebra is a ring A with identity together with a ring homomorphism $f: R \to A$ mapping 1_R to 1_A such that the subring $f(R)$ of A is contained in the center of A

Naturally A has both LEFT AND RIGHT R-module structure given by

$$r \cdot a = a \cdot r = \underbrace{f(r)a = af(r)}$$

$f(r) \in Z(A) = \text{Center}(A)$

$Z(A) = \{ b \in A \mid bx = xb \ \forall x \in A \}$

Next, define homomorphism of R-algebras and isomorphism of such objects,

Def^{n}/ If A and B are two R-algebras, an R-algebra homomorphism is a ring homomorphism $\varphi: A \to B$ mapping 1_A to 1_B such that $\varphi(r \cdot a) = r \cdot \varphi(a)$ for all $r \in R$ and $a \in A$. Likewise an isomorphism of R-algebras is a homomorphism of R-algebras which is a bijection.

Examples of R-algebras

We continue to assume R is ring with 1.

$\boxed{\text{E1}}$ $R = \mathbb{Z}_2 = \{0,1\}$ is $\mathbb{Z}$-algebra

(1.) R is a $\mathbb{Z}$-algebra

(2.) If A has subring R contained in center of the ring with identity A then A forms an R-algebra

$R[x]$ is an R-algebra

$R[x,y]$ is an R-algebra

RG the group ring is an R-algebra

$R^{n \times n}$ is an R-algebra

each example above contains R in the center of the ring* and in practice we sometimes identify that copy of R with R on its lonesome

$\mathbb{C}$ is a $\mathbb{R}$-algebra

$\mathbb{H}$ is a $\mathbb{C}$-algebra

See $\boxed{\text{E1}}$ for instance

Remark: $f : R \longrightarrow A$ a ring homomorphism we don't always have $f(R)$ isomorphic to R, I'm not correct at * unless $\ker(f) = 0$. Recall R = field forces nontrivial ring homomorphism $f : R = F \longrightarrow A$ to be injective

Th^m/ An F-algebra contains an isomorphic copy of the field F in the center of the algebra

QUOTIENT MODULES AND MODULE HOMOMORPHISMS

The def^{n} below naturally extends the theory of vector spaces and linear transformations to R-modules and R-mod. homomorphisms.

Def^{n}/ Let R be a ring and M and N be R-modules

(1.) A map $\varphi: M \longrightarrow N$ is an <u>R-module homomorphism</u> if it respects the R-module structures of M & N,

(a.) $\varphi(x+y) = \varphi(x) + \varphi(y) \quad \forall x, y \in M$

(b.) $\varphi(rx) = r\varphi(x) \quad \forall r \in R, x \in M.$

(2.) An R-module homomorphism is an <u>isomorphism</u> of R-modules if it is both injective and surjective. The modules M and N are <u>isomorphic</u>, denoted $M \cong N$, if $\exists$ R-module isomorphism $\varphi: M \longrightarrow N$

(3.) If $\varphi: M \longrightarrow N$ is an R-module homomorphism, let $\ker\varphi = \{m \in M \mid \varphi(m) = 0\}$ (kernel of φ) and let $\varphi(M) = \{n \in N \mid n = \varphi(m) \text{ for some } m \in M\}$ (the image of φ)

(4.) Let M and N be R-modules and define $\text{Hom}_R(M,N)$ to be set of all R-module homomorphisms from M into N.

<u>Remark</u>:

<u>R-modules</u>		<u>$\mathbb{F}$-vector spaces</u>
R	$\longrightarrow$	$\mathbb{F}$
M	$\longrightarrow$	$V(\mathbb{F})$
$\varphi: M \to N$	$\longrightarrow$	$T: V \to W$
$\text{Hom}_R(M,N)$	$\longrightarrow$	$\mathcal{L}_{\mathbb{F}}(V,W)$

Exercise for Reader: show $\ker \varphi$ and $\operatorname{im} \varphi$ are R-submodules given $\varphi \in \operatorname{Hom}_R(M,N)$ for M, N R-modules.

Examples

(1.) $M = R$ is an R-module, but beware $\varphi \in \operatorname{Hom}_R(R,R)$ need not be ring homomorphism.

(a.) $R = \mathbb{Z}$, $\varphi(x) = 2x$
$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$

$$\varphi(x+y) = 2(x+y) = 2x + 2y = \varphi(x) + \varphi(y)$$
$$\varphi(nx) = 2(nx) = n(2x) = n\varphi(x)$$

However, $\varphi(1) = 2$ thus φ not a ring homomorphism for the unital ring $\mathbb{Z}$.

(b.) $R = F[x]$, $\varphi(f(x)) = f(x^2)$
$\varphi : F[x] \longrightarrow F[x]$

$$\varphi(f(x) + g(x)) = f(x^2) + g(x^2) = \varphi(f(x)) + \varphi(g(x))$$
$$\varphi(r(x)f(x)) = r(x^2)f(x^2) \neq r(x)\varphi(f(x))$$

φ not a $R = F[x]$-module homomophism

YET, $\varphi(r(x)f(x)) = \varphi(r(x))\varphi(f(x))$ and $\varphi(1) = 1$, here φ <u>is</u> a <u>ring</u> <u>homomorphism</u> but is not an $\mathbb{F}[x]$-module homomorphism.

(contrast)

RING HOMOMORPHISM

$\varphi : R \rightarrow S$
$\varphi(x+y) = \varphi(x) + \varphi(y)$
$\varphi(xy) = \varphi(x)\varphi(y)$
$\varphi(1) = 1$

R-module HOMOMORPHISM

$\varphi : M \rightarrow N$
$\varphi(x+y) = \varphi(x) + \varphi(y)$
$\varphi(r \cdot x) = r \cdot \varphi(x)$

(2.) Suppose R a ring and $n \in \mathbb{Z}^+ = \mathbb{N}$ and construct $M = R^n = \{(x_1, .., x_n) \mid x_i \in R\}$

Def^n/ $\pi_i : R^n \longrightarrow R$ is the <u>projection map</u> onto i^{th} coordinate,

$$\pi_i(x_1, .., x_n) = x_i$$

you can verify that π_i is surjective and $\pi_i \in \mathrm{Hom}_R(R^n, R)$ and

$$\ker \pi_i = \underbrace{R \times R \times \cdots \times \{0\} \times \cdots \times R}_{\{0\} \text{ in } i^{th} \text{ slot.}}$$

(3.) $R = \mathbb{F}$ a field then R-module homomorphisms are linear transformations of vector spaces.

(4.) $R = \mathbb{Z}$ the condition $\varphi(n \cdot x) = n \cdot \varphi(x)$ is automatically given from $\varphi(x+y) = \varphi(x) + \varphi(y)$ for instance $\varphi(1+1) = \varphi(2 \cdot 1) = 2 \cdot \varphi(1)$ well more to point, $\varphi(2 \cdot x) = \varphi(x+x) = \varphi(x) + \varphi(x) = 2 \cdot \varphi(x)$ etc.

Th^m/ $\mathbb{Z}$-module homomorphisms are the same as abelian group homomorphisms

(5.) Let R be a ring and I a two-sided ideal which $\underbrace{\text{annihilates}}$ R-modules M and N

$$\left\{\begin{array}{ll} am = 0 & \text{for all } a \in I,\ m \in M \\ an = 0 & \text{for all } a \in I,\ n \in N \end{array}\right)$$

Then if $\varphi : M \to N$ is an R-mod. homomorphism naturally viewed $\varphi : M \to N$ as an (R/I)-module homomorphism.

<u>application</u> : Given $\varphi : M \to N$ a $\mathbb{Z}$-module homomorphism if $(p) = p\mathbb{Z}$ annihilates both M and N then φ defines a $(\mathbb{Z}/p\mathbb{Z})$-module homomorphism.

<u>application</u> : if A is abelian group for which $px = 0$ $\forall x \in A$ for some prime $p \in \mathbb{N}$ then any group homomorphism $\varphi : A \to A$ is a $(\mathbb{Z}/p\mathbb{Z})$-module homomorphism on A.

For instance, $B = \mathrm{Aut}(A)$ gives $\varphi \in B$ $\varphi : A \to A$ invertible group homomorphism

$$\Rightarrow \varphi \in \mathcal{L}_{\mathbb{F}_p}(A, A) = \mathrm{Hom}_{\mathbb{Z}/p\mathbb{Z}}(A, A)$$

$$\mathrm{Aut}(A) = GL(A).$$

Proposition 2

Let M, N and L be R-modules

(1.) A map $\varphi : M \longrightarrow N$ is R-module homomorphim iff $\varphi(rx+y) = r\varphi(x) + \varphi(y)$ $\forall x, y \in M, r \in R$.

(2.) $\mathrm{Hom}_R(M,N)$ is an R-module given the natural definitions for $\mathrm{Hom}_R(M,N)$ (see below) and that R is <u>commutative</u> ring.

(3.) $\varphi \in \mathrm{Hom}_R(L,M)$ and $\psi \in \mathrm{Hom}_R(M,N)$ then $\psi \circ \varphi \in \mathrm{Hom}_R(L,N)$.

(4.) $\mathrm{Hom}_R(M,M)$ is ring with 1 using function addition as $+$ and function composition as multiplication. When R commutative, <u>$\mathrm{Hom}_R(M,M)$ is an R-algebra</u>.

The natural definitions for addition and R-multiplication for $\varphi, \psi \in \mathrm{Hom}_R(M,N)$ are given by usual <u>pointwise definined</u> maps, <u>assume R commutative ring</u>

$$(\varphi + \psi)(x) \overset{\mathrm{def}^n}{=\!=} \varphi(x) + \psi(x) \qquad \forall x \in M$$

$$(r\varphi)(x) \overset{\mathrm{def}^n}{=\!=} r\varphi(x) \qquad \forall x \in M, r \in R$$

Proof of Proposition 2 is routine, we'll just look at a portion of the proof (p. 347 of D&F)

$$\begin{aligned}
(r_1\varphi)(r_2 m) &= r_1\varphi(r_2 m) && : \text{def}^{\underline{n}} \text{ of } r_1\varphi \\
&= r_1 r_2 \varphi(m) && : \varphi \text{ is } R\text{-mod. homomorphism} \\
&= r_2 r_1 \varphi(m) && : R \text{ commutative} \\
&= r_2 (r_1\varphi)(m) && : \text{def}^{\underline{n}} \text{ of } r_1\varphi
\end{aligned}$$

This shows $r_1\varphi$ has the property (6.) for R-mod. homomorphism.

PART OF proof for (3.) given $\varphi : L \to M$ and $\psi : M \to N$ both R-module homomorphisms then $\psi \circ \varphi : L \xrightarrow{\varphi} M \xrightarrow{\psi} N$ has,

$$\begin{aligned}(\psi \circ \varphi)(rx+y) &= \psi(\varphi(rx+y)) \\ &= \psi(r\varphi(x)+\varphi(y)) \\ &= r\,\psi(\varphi(x)) + \psi(\varphi(y)) \\ &= r(\psi\circ\varphi)(x) + (\psi\circ\varphi)(y)\end{aligned}$$

thus $\psi \circ \varphi$ satisfies (a) and (b.) of axioms for R-module homomorphism (using (1.) which is almost obvious)

(4.) $\varphi, \psi \in \mathrm{Hom}_R(M,M)$ then $\varphi \circ \psi : M \to M$, thus $\circ$ defines binary operation on $\mathrm{Hom}_R(M,M)$ and $\varphi + \psi \in \mathrm{Hom}_R(M,M)$ as well, anyway $\mathrm{Hom}_R(M,M)$ is an Ring with identity.
Notice $1 = Id_M$ defined by $Id_M(x) = x \quad \forall x \in M$ gives $1 \circ \varphi = \varphi = \varphi \circ 1$ for all $\varphi \in \mathrm{Hom}_R(M,M)$ and we can check $\mathrm{Hom}_R(M,M)$ forms a <u>ring</u> (usually not commutative)

Defn/ R commutative then $\mathrm{Hom}_R(M,M)$ gives LEFT R-module for a given R-module M via

$$\varphi r = r\varphi \quad \text{for all } \varphi \in \mathrm{Hom}_R(M,M)$$

Defn/ $\mathrm{End}_R(M) = \mathrm{Hom}_R(M,M)$ is endomorphism ring of M, $\varphi \in \mathrm{End}_R(M)$ is an endomorphism

The ring of endomorphisms for a module M over a <u>commutative</u> ring R is naturally an R-module via

$$(r\varphi)(x) = r\varphi(x)$$

for each $r \in R$ and $\varphi \in \mathrm{Hom}_R(M,M) = \mathrm{End}_R(M)$. We can show $\mathrm{End}_R(M)$ is an <u>R-algebra</u> in this case, construct $f : R \longrightarrow \mathrm{End}_R(M)$

$$f(r) = r\,\mathrm{Id}_M$$

and observe $(r\,\mathrm{Id}_M)\circ\varphi = \varphi\circ(r\,\mathrm{Id}_M)$ $\forall \varphi \in \mathrm{End}_R(M)$ thus $f(R)$ is within the center of $\mathrm{End}_R(M)$.

Defn/ the endomorphisms of the form $r\,\mathrm{Id}_M$ are the <u>scalar</u> <u>multiplications</u> of $\mathrm{End}_R(M)$

(perhaps we should reserve this terminology to the case $R = \mathbb{F}$ a field)

<u>Remark</u>: $f(R) \cong R$ gives copy of R within $\mathrm{End}_R(M)$ in the case $R = \mathbb{F}$ a field. We can identify the field as scalar multiples of the <u>identity</u> <u>transformation</u> in $\mathrm{End}_R(M)$.

PROPOSITION 3

Let R be a ring, let M be an R-module and N a submodule of M. The (additive abelian) quotient group M/N can be made into an R-module by defining

$$r(x+N) = (rx)+N \quad \text{for all } r \in R,\ x+N \in M/N$$

and the natural projection map $\pi : M \longrightarrow M/N$ defined by $\pi(x) = x+N$ is an R-module homomorphirm with $\ker \pi = N$.

Proof: since N is subgroup of M w.r.t. abelian $+$ it follows N is normal (additive) subgroup of M hence $M/N = \{x+N \mid x \in M\}$ gives well-defined operations $(x+N)+(y+N) = (x+y)+N$ making M/N an abelian group w.r.t coset addition. I'll leave well-defined as exercise to reader, let's focus here on the R-module structure,

$$\begin{aligned}(r_1r_2)(x+N) &= (r_1r_2x)+N \\ &= r_1(r_2x+N) \\ &= r_1(r_2(x+N))\end{aligned}$$

(axiom 6 of R-module verified for M/N)

other axioms can be checked similarly.

Def^{n}/ Let A, B be submodules of the R-module M. The <u>sum</u> of A and B is $A+B = \{a+b \mid a \in A, b \in B\}$

Proposition: $A+B$ as above is a submodule of M.

<u>Proof:</u> $0 \in A$ and $0 \in B$ since A, B submodules therefore $0 = 0 + 0 \in A+B \neq \emptyset$. Suppose $x, y \in A+B$ and $r \in R$ then $\exists\, a_x, a_y \in A$ and $b_x, b_y \in B$ for which $x = a_x + b_x$ and $y = a_y + b_y$

Thus,

$$\begin{aligned} rx + y &= r(a_x + b_x) + a_y + b_y \\ &= r(a_x + a_y) + b_x + b_y \\ &= ra + b \in A+B. \end{aligned}$$

$r(a_x+a_y) = a \in A$
$b_x + b_y = b \in B$
using R-module properties of A and B

Hence $A+B$ is submodule by the submodule criterion.

Th^{m}(4) (FIRST, SECOND, THIRD ISOMORPHISM TH^{m}'s FOR MODULES)

(1.) M, N R-modules and $\varphi : M \to N$ an R-module homomorphism. Then $\ker\varphi$ is submodule of M and $M/\ker\varphi \cong \varphi(M)$

(2.) A, B submodules of M then $\dfrac{A+B}{B} \cong \dfrac{A}{A \cap B}$

(3.) M an R-module and A, B submodules of M with $A \subseteq B$ then

$$\frac{M/A}{B/A} \cong \frac{M}{B}$$